## ABSTRACT OF THE DISCLOSURE

A signal processing apparatus for performing modular multiplication for use in a signal processing system includes a first logic for outputting a signed multiplicand by selectively performing a one's complementary operation on a multiplicand according to a Booth conversion result of a multiplier in modular multiplication; a second logic for outputting a modulus which is signed in the modular multiplication based on a carry input value Carry-in of a current clock, determined from a carry value cin for correction of a previous clock, and on a sign bit of the multiplicand; and a third logic for receiving the signed multiplicand and the signed modulus, and calculating a result value of the modular multiplication by iteratively performing a full addition operation on a carry value C and a sum value S of the full addition operation, found at the previous clock. The present invention provides a high-speed modular multiplication apparatus with fewer gates and reduced power consumption.